

Insecure primitive elements in an ElGamal signature protocol

Omar Khadir

Laboratory of Mathematics, Cryptography and Mechanics, Fstm
University Hassan of Casablanca, Morocco
e-mail: khadir@hotmail.com

Abstract

Consider the classical ElGamal digital signature scheme based on the modular relation $\alpha^m \equiv y^r r^s \pmod{p}$. In this work, we prove that if we can compute a natural integer i such that $\alpha^i \pmod{p}$ is smooth and divides $p - 1$, then it is possible to sign any given document without knowing the secret key. Therefore we extend and reinforce Bleichenbacher's attack presented at Eurocrypt'96.

Keywords : ElGamal signature scheme, public key cryptography, cryptanalysis.

MSC 2010 : 94A60

1 Introduction

It was in 1976 that Diffie and Hellman published their famous paper "New directions in cryptography" [4]. For the first time in communication history, they provided us with a mechanism that guarantees the confidentiality of documents and data we like to exchange over a public and insecure channel. This event is at the origin of the public key cryptography [4,14,13]. Since then, many original cryptographical methods were conceived and proposed to solve a variety of communication problems like identification, authentication, integrity or 0-knowledge proof. However, the most important field in public key cryptography is probably the digital signature protocol. Its requirement in e-business for funds transferring, makes it a sensitive question. Let us recall the principle. For the user Alice we prepare two kind of keys. The first, y , is public and must be largely diffused to the other users. The second, x , is private and must be kept secret. When Alice decides to sign a document M , she has to solve a difficult problem, in general a mathematical equation. This problem

is depending of Alice public key y and of the document M . It is constructed in a way such that nobody, except Alice, can solve it. With the help of her secret key x , Alice is able to give the answer.

The equation is based on a hard question in mathematics like factorization or discrete logarithm problem. We cannot forge Alice signature, but anyone like a judge can verify that the solution she gives is valid.

Let p be a prime number and α a primitive element modulo p . The discrete logarithm problem consists of solving the modular equation $\alpha^x \equiv \beta \pmod{p}$, where β is a fixed integer and x is the unknown variable. In 1978, Pohlig and Hellman [12] elaborated an efficient algorithm when $p - 1$ is B -smooth. In 1985, ElGamal [6] proposed a public key cryptosystem and one of the first digital signature protocols both based on the discrete logarithm. Nobody knows how he found his difficult signature equation. Several variants of the signature scheme were developed [15, 5, 10 table 11.5 p.457,7,9]. In 1996, Bleichenbacher [2,3] built an attack that relies on Pohlig and Hellman algorithm if ElGamal signature parameters are not properly chosen. In 1999, Kuwakado and Tanaka [9] proved that, when we use ElGamal method to sign two documents, if the secret nonces k_1, k_2 are less than the square root of the prime modulus p , then we can compute the secret key of the signer and break all the system. In 2011, the author slightly extended Bleichenbacher's attack [8].

Let $\alpha^m \equiv y^r r^s \pmod{p}$ be the ElGamal classical signature equation. In this work, we show that if we can compute a natural integer i such that $\alpha^i \pmod{p}$ is B -smooth and divides $p - 1$, then it is possible to sign any given document without knowing the secret key. As a consequence, we prove that if (p, α, y) is Alice public key, and if one the four positive integers α , $p - \alpha$, $\frac{1}{\alpha} \pmod{p}$ or $-\frac{1}{\alpha} \pmod{p}$ is B -smooth and divides $p - 1$, then it is possible to sign any message without knowing Alice private key. Therefore we extend and reinforce Bleichenbacher's attack presented at Eurocrypt'96.

Note also, that our work tends to confirm, what was mentioned by many authors: it is certainly easier to break ElGamal signature scheme than to solve the discrete logarithm problem.

Our paper is organized as follows. In section 2 we briefly recall the classical ElGamal signature scheme. Section 3 is devoted to the review of Bleichenbacher's

attack [2,3]. Our contribution is presented in section 4. We conclude in section 5.

Throughout this article, we will adopt ElGamal paper notations [5]. \mathbb{Z} , \mathbb{N} are respectively the sets of integers and non-negative integers. For every positive integer n , we denote by \mathbb{Z}_n the finite ring of modular integers and by \mathbb{Z}_n^* the multiplicative group of its invertible elements. Let a, b, c be three integers. The great common divisor of a and b is denoted by $\gcd(a, b)$. Two numbers a and b are said to be coprime if $\gcd(a, b) = 1$. We write $a \equiv b [c]$ if c divides the difference $a - b$, and $a = b \bmod c$ if a is the remainder in the division of b by c . The positive integer a is said to be B -smooth [10, p.92], $B \in \mathbb{N}$, if every prime factor of a is less than or equal to the bound B . Generally, parameter B depends of the computer power.

2 Classical ElGamal signature

In this section we recall the basic ElGamal signature scheme [6, 16 p.287, 10 p.454, 11 p.183].

1. Alice chooses three numbers:

- p , a large prime integer.
- α , a primitive element (or a generator) [10, p.69] of the finite multiplicative group \mathbb{Z}_p^*
- x , a random element belonging to the set $\{2, 3, \dots, p - 2\}$.

Then she computes $y = \alpha^x \bmod p$. Alice public keys are (p, α, y) , and x is her private key.

2. To sign the message m , Alice needs to solve the equation :

$$\alpha^m \equiv y^r r^s [p] \quad (1)$$

where r, s are the unknown variables.

Alice fixes arbitrary r to be $r = \alpha^k \bmod p$, where k is chosen randomly and invertible modulo $p - 1$. Equation (1) is then equivalent to :

$$m \equiv xr + ks [p - 1] \quad (2)$$

As Alice knows the secret key x , and as the integer k is invertible modulo $p - 1$, she computes the second unknown variable s : $s \equiv \frac{m - xr}{k} [p - 1]$

3. Bob can verify the signature by checking that congruence (1) is valid for the variables r and s given by Alice.

To avoid some attacks, instead of signing a message M , it is more secure to apply a hash function h , like SHA1 [16 p.137, 10 p. 348], and compute $m = h(M)$ before signing the hashed value m .

3 Bleichenbacher's attack

In this part we recall Bleichenbacher's remarkable attack presented at the Eurocrypt'96 conference [2]. Here, of course, we use the corrected version [3].

Let (p, g, y_A) be Alice public key in an ElGamal signature scheme, and x_A his private key.

Theorem 1. [3] let $p - 1 = bw$ where b is smooth and let $y_A \equiv g^{x_A} \pmod{p}$ be the public key of user A. If r and k are known such that $r \equiv \alpha^k \equiv cw \pmod{p}$ with $0 < c < b$ then it is possible to generate a valide ElGamal signature (r, s) for all h with $h \equiv x_A r \pmod{\gcd(k, p - 1)}$ can be found. In particular when r is a generator of \mathbb{F}_p^* then it is possible to generate an ElGamal signature for all h .

Theorem 1 has an immediate practical consequence :

Corollary 1. ([3]) If α is B -smooth and divides $p - 1$ then it is possible to generate a valid ElGamal signature on an arbitrary value h if $p \equiv 1 \pmod{4}$ and on one half of the values $0 \leq h < p$ if $p \equiv 3 \pmod{4}$.

when $p \equiv 1 \pmod{4}$, we easily derive the following algorithm and we will exploit it in an illustrative example of our own attack.

Algorithm 1.

- 1- Input (p, α, y) ; $\{\alpha$ is B -smooth and divides $p - 1$, $p \equiv 1 \pmod{4}\}$
- 2- Input m ; $\{m = h(M)$ where M is the message to be signed. $\}$
- 3- $k \leftarrow (p - 3)/2$;
- 4- $r \leftarrow \alpha^k \pmod{p}$; $\{ r$ is is the first parameter of the digital signature. We also have $r := (p - 1)/\alpha. \}$
- 5- $w \leftarrow (p - 1)/\alpha$;
- 6- $b \leftarrow \alpha^w \pmod{p}$; $\{b$ is a generator of a suitable subgroup $H\}$.
- 7- $B \leftarrow y^w \pmod{p}$; $\{B$ is an other element of $H\}$.

- 8- $x_0 \leftarrow x$; { x is a solution to the easy discrete logarithm problem $b^x \equiv B \pmod{p}$, since the Pohlig and Hellman algorithm [12] is efficient. }
- 9- $s \leftarrow \frac{h(M) - rx_0}{k} \pmod{p-1}$; { s is the second parameter of the digital signature. }
- 10- Output (r, s) . { The couple (r, s) is the ElGamal digital signature without using Alice private key x . }

In 2011, Corollary 1 was extended by the author to the next more general result:

Theorem 2. [8] Let (p, α, y) be Alice public key in an ElGamal signature protocol. An adversary can forge Alice signature for any given message if one of the following conditions is satisfied :

- a) $p \equiv 1 \pmod{4}$, α is B-smooth and divides $p - 1$.
- b) $p \equiv 1 \pmod{4}$, $\frac{1}{\alpha} \pmod{p}$ is B-smooth and divides $p - 1$.
- c) α^2 is B-smooth and divides $p - 1$.

4 Our contribution

We start this section by describing our main result which is a significant extension of Bleichenbacher's Corollary 1. Throughout this part, for more clarity and without loss of generality, we always suppose that the prime modulus p is equivalent to 1 modulo 4. When $p \equiv 3 \pmod{4}$ all our results still valid but only for documents M such that the integer $m = h(M)$ has a fixed parity.

Theorem 3. Let (p, α, y) be Alice public key in an ElGamal signature protocol. Suppose that $p \equiv 1 \pmod{4}$. If we can compute a natural integer i , coprime to $p - 1$, such that $\alpha^i \pmod{p}$ is B-smooth and divides $p - 1$, then it is possible to generate a digitale signature for any given document without knowing Alice private key.

Proof. Let M be the message that we would like to sign and $m = h(M)$ be its hashed value. We must find two unknown integers r and s such that $\alpha^m \equiv y^r r^s \pmod{p}$. Let i be a natural integer coprime to $p - 1$ such that $\alpha^i \pmod{p}$ is B-smooth and divides $p - 1$. ElGamal digital signature Equation (1) is equivalent to

$$\alpha^{im} \equiv y^{ir} r^{is} \pmod{p} \quad (3)$$

If we set $\beta = \alpha^i \pmod{p}$, $z = y^i \pmod{p}$, $u = r$ and $v = is \pmod{p-1}$, we obtain the new modular equation

$$\beta^m \equiv z^u u^v \pmod{p} \quad (4)$$

Since $\gcd(i, p-1) = 1$, the element $\beta^i \bmod p$ is a primitive root. As $\beta^x \bmod p = z$, where x is Alice secret key, the triplet (p, β, z) can be seen as the public key of an imaginary user in an ElGamal signature protocol. We do not need the private key x . For any given document M , by Corollary 2, it is possible to solve equation (4) and to find the unknown variables u and v . Therefore, we generate a signature by giving the couple $r = u$ and $s = \frac{v}{i} \bmod (p-1)$.

□

Observe that a trapdoor could be hidden in the generator α by choosing it such that $\alpha^i \bmod p$ is B -smooth and divides $p-1$, with a large exponent i .

To illustrate our technique, let us give a numerical example.

Example 1. Assume that $p = 1597$, $\alpha = 11$ and $y = 159$. The secret key $x = 856$ is ignored.

Suppose that we want to sign the message M such that $m = h(M) = 1234$, where h is a hash function like SHA1. Observe, first, that Bleichenbacher's attack cannot be mounted here. On another side, conditions a) and b) in Theorem 2 are not satisfied. Let us therefore apply our method. With the help of a computer, we find that the smallest positive exponent i such that $\beta = \alpha^i \bmod p$ divides $(p-1)$ is $i = 275$. As $z = y^i \bmod p = 1287$, we determine the public key of a fictive user $(p, \beta, z) = (1597, 38, 1287)$. Obviously β is B -smooth. Algorithm 1 gives us the signature $(u, v) = (42, 1202)$. As $u = r$ and $v = is \bmod (p-1)$, we obtain $(r, s) = (42, 370)$. So, we have signed the message M such that $h(M) = 1234$ without using Alice private key x . Any verifier can check that the ElGamal modular equation (1) is valid.

Assume that (p, α, y) is Alice public key. In somehow, our result in Theorem 3 means that, to break the ElGamal digital signature system, it is not needed to have $p-1$ a multiple of α as it is claimed by Bleichenbacher [2,3], but it suffices to have $p-1$ a multiple of anyone of the primitive elements modulo p . Next corollary is another extension.

Corollary 2. Let (p, α, y) be Alice public key in an ElGamal signature protocol. Suppose that $p \equiv 1 \pmod{4}$. If one among the four positive numbers α , $p - \alpha$, $\frac{1}{\alpha} \bmod p$ or $\frac{-1}{\alpha} \bmod p$, is B -smooth and divides $p-1$, then it is possible to generate a

signature for any given document without knowing Alice private key.

Proof. For α and $\frac{1}{\alpha} \bmod p$ apply respectively Corollary 1 and Theorem 2. Let us study the two cases corresponding to $p - \alpha$ and $-\frac{1}{\alpha} \bmod p$. The even integer $p - 1$ can be decomposed as $p - 1 = 2^k l$, where k, l are the two easily computable natural numbers such that $k \geq 2$ and l is odd. Fermat little theorem gives the modular relation $\alpha^{p-1} \equiv 1 [p]$. As the order of the primitive element α is $p - 1$, looking at the factorization of $\alpha^{p-1} - 1$ modulo p , we necessary have $\alpha^{2^{k-1}l} \equiv -1 [p]$ which implies $\alpha^{2^{k-1}l+1} \equiv -\alpha [p]$ and $\alpha^{2^{k-1}l-1} \equiv -\frac{1}{\alpha} [p]$. Since $\gcd(\alpha^{2^{k-1}l \pm 1}, p - 1) = 1$, the proof is achieved by immediate application of our theorem 3.

□

There is a well known particular situation for the generator choice: "Choosing $\alpha = 2$ is exceptionally bad" [2,3,1,10 p.456]. We extend the case:

Corollary 3. Let (p, α, y) be Alice public key in an ElGamal signature protocol. Suppose that $p \equiv 1 [4]$. It is possible to forge Alice digital signature for any given message M if we have one of the two conditions:

- i) $\alpha = 2$.
- ii) Number 2 is a primitive element of the multiplicative group \mathbb{Z}_p^* and the positive exponent i such that $\alpha^i \equiv 2 [p]$ is computable.

Proof. Similar to the justification of Theorem 3.

□

5 Conclusion

In this paper, we determined new primitive elements of the multiplicative finite group \mathbb{Z}_p^* , p prime, for which ElGamal digital signature scheme is no more secure. We therefore made an extension of the old and remarkable result presented by Bleichenbacher at Eurocrypt'96.

References

- [1] R. Anderson, S. Vaudenay *Minding your p's and q's*, In Advances in Cryptology, Asiacrypt'96, LNCS 1163, Springer-Verlag, (1996), pp. 26 – 35.

- [2] D. Bleichenbacher, *Generating ElGamal signatures without knowing the secret key*, In Advances in Cryptology, Eurocrypt'96, LNCS 1070, Springer-Verlag, (1996), pp. 10 – 18.
- [3] D. Bleichenbacher, *Generating ElGamal signatures without knowing the secret key* (1996).
Available at <ftp://ftp.inf.ethz.ch/pub/crypto/publications/Bleich96.pdf>
- [4] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, Vol. IT-22, (1976), pp. 644-654.
Available at <http://www.cs.tau.ac.il/~bchor/diffie-hellman.pdf>
- [5] DSA. National institute of standard and technology (NIST). FIPS Publication 186, Department of commerce, 1994.
Available at <http://www.itl.nist.gov/fipspubs/fip186.htm>
- [6] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithm problem*, IEEE Trans. Info. Theory, IT-31, (1985), pp. 469 – 472.
Available at <http://groups.csail.mit.edu/cis/crypto/classes/6.857/papers/elgamal.pdf>
- [7] P. HORSTER, M. MICHELS, H. PETERSEN, *Generalized ElGamal signature schemes for one message block*, Technical Report, TR-94-3, (1994).
- [8] O. Khadir, *Conditions on the generator for forging ElGamal signature*, Int. J. P. Applied Math., Vol. 70, no. 7, (2011), pp. 939 – 949.
Available at <http://www.ijpam.eu/contents/2011-70-7/5/5.pdf>
- [9] H. Kuwakado and H. Tanaka. *On the security of the ElGamal-type signature scheme with small parameters*, IEICE Trans. Fundamentals Electron. Commun. Comput. Sci., 1999, E82, pp. 93 – 97.
- [10] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, Florida, (1997).
Available at <http://www.cacr.math.uwaterloo.ca/hac/>
- [11] A. R. Mollin, *An introduction to cryptography*, Chapman & Hall/CRC, (2007), Second Edition. (1997).

- [12] S. C. Pohlig, M. E. Hellman, *An improved algorithm for computing logarithms over $\text{GF}(p)$ and its cryptographic significance*, IEEE Trans. Information Theory IT-24 (1978), no. 1, pp. 106 – 110.
- [13] M. O. Rabin, *Digitalized signatures and public key functions as intractable as factoring*, MIT/LCS/TR, Vol. 212, 1979.
- [14] R. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Communication of the ACM, Vol. no 21, (1978), pp. 120 – 126.
- [15] C. P. Schnorr, *Efficient signature generation by smart cards*, J. of Cryptology, (1991), pp. 161 – 174.
- [16] D. R. Stinson, *Cryptography, theory and practice*, Third Edition, Chapman & Hall/CRC, (2006).